TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Arvutiteaduse instituut

Ründed juhtmevabadele sensorvõrkudele

Kodutöö aines „Infosüsteemide ründed ja kaitse“

Koostanud:
Romi Agar 040719

Tallinn 2008

Sisukord

Sissejuhatus

Juhtmevaba sensorvõrk (ingl k *Wireless Sensor Network – WSN*) koosneb hulgast väikestest seadmetest, millel võivad küljes olla erinevad andurid. Selliselt moodustunud võrk saab täita erinevaid tööülesandeid kui võrgusõlmed suhtlevad üksteisega raadio teel. Tänapäeval leiavad sensorvõrgud üha laialdasemat kasutust nii uurimusprojektides, kommertslahendustes kui ka kaitseprojektides. WSN kasutusalad ulatuvad sissetungi tuvastusest ja tootmisliinide jälgimisest kuni looduselustiku jälgimiseni välja ning inimesed leiavad pidevalt üha uusi rakendusi sensorvõrkudele.

Luues aga uusi rakendusi võib kergesti ära unustada sensorvõrgu turvalisuse küsimuse. Mõnede jaoks on sportlik huvi leida nõrkusi, ärakasutamisvõimalusi ja vigu kõiges, mis hõlmab endas nii raud- kui tarkvara, kuid sõltuvalt sensorvõrgu ülesandest võib see motivatsioon osutuda hoopistükkis kuritegelikumaks. Et seda ei juhtuks, on kasulik teada, kuidas sensorvõrkude raudvara ja tarkvara peavad vastu erinevatele ründe tüüpidele.

Kaabelvõrkude ehk juhitud meediaga võrkude pealtkuulamine ja ründamine on palju raskem kui vaba levikeskkonnaga juhtmevabadel võrkude puhul. Juhtmevabade tehnoloogiate olemuse kombinatsioon koos üha harituma kasutajaskonnaga tagab vaenlastele üha kergema juurdepääsu sensorseadmetevahelisele kommunikatsioonile. Ainsaks eelduseks on vastava raadiovastuvõtja/-saatja olemasolu, mis on aga üsnagi odavalt soetatav.

WSN turvalisuse temaatikat võib mõneti võrrelda WiFi võrku omaga, sest tegu on samuti juhtmevaba tehnoloogiaga, pealegi mõlemad töötavad samas sagedusvahemikus ka. Kui arvestada seda, et on tõestatud praegugi veel üsna laialdaselt kasutuses oleva WEP krüpteeringu kergesti murtavus [1] ning ka WPA krüpteeringu nõrgad küljed [2] ja ka see, et WiFi seadmetel on püsitoiteallikad, suurem arvutusvõimsus ning väiksemad hinnapiirangud kui arupuru kübemetel, siis on sensorvõrkude turvalisuse küsimus vägagi murettekitav. Lisaks on arupuru kübemete juures üsnagi kiusatuslik teha järeleandmisi turvalisuses pikenenud patareieluea, väiksemate füüsiliste mõõtemete ning maksumuse vastu, mis omakorda tekitab väljakutseid.

Ründed sensorvõrkude vastu võivad leida aset erinevatel kommunikatsioonikihtidel ning sellest lähtuvalt ja arvestades kõiki sensorvõrkude poolt seatud piiranguid on taoliste võrkude kaitseks välja pakutud erinevaid meetodeid. Järgnevalt püüaksingi vaadata erinevatel võrgukihtidel toimuda võivaid ründetüüpe koos võimalike kaitsemeetmetega, alustades kõige madalamast – füüsilisest – kihist ning liikudes kommunikatsioonimudeli kihilises struktuuris üles poole kuni võrgukihi ja ruutimisprotokollide rünneteni välja. Kuid kõigepealt vaatame pisut probleemi püstitust.

Probleemi püstitus

Siin kirjeldame laialt levinud ohumudelit ning usaldusmudelit koos turvalisuse eesmärkidega sensorvõrkudes.

Ohumudel

Üldiselt võib ründeid kategoriseerida järgnevalt [17]:

- ***kübeme klassi* ründaja** vs. ***sülearvuti tüüpi* ründaja:** Kübeme klassi ründajal on juurdepääs üksikutele kübemetele, kellel kõigil on sama tüüpi võimalused ning piirangud. Süleri tüüpi ründajal on juurdepääs palju võimsamatele seadmetele, mis annab talle eelise ja võimaluse teostada palju suurema ulatusega ja tõsidusega ründeid.
- ***siseinfo valdaja* rünne** vs ***kõrvalise isiku* rünne**: Autsaiderist ründajal ei ole spetsiaalset juurdepääsu võrku, tema saab põhimõtteliselt passiivselt võrguliiklust salaja pealt kuulata. Samas siseinfo valdajal on juurdepääs krüpteerimisvõtmetele ning muule võrgu siseinfole.
- ***passiivne* rünne** vs ***aktiivne* rünne**: Passiivne ründaja on reeglina huvitatud sensitiivse info kogumisest sensorvõrgust, mis kompromiteerib turvalisuse privaatsuse ja konfidentsiaalsuse nõuet. Passiivne ründaja kuulab peal võrguliiklust ning analüüsib saadud infot, et ekstraheerida sealt välja endale vajalik teave, mida võib hiljem kasutada näiteks aktiivse ründe teostamiseks. Aktiivse ründe eesmärk on võrgu toimimise segamine ja jõudluse alandamine. Põhilised aktiivründed on teenusetõkestusründed (ingl k *Denial of Service attacks – DoS attacks*)

Usaldusmudel

Sensorvõrkudes on reeglina üks kuni mitu baasjaama nagu näiteks personaalarvutid, kuhu kogu võrgu poolt kogutud ja töödeldud info kokku kogutakse. Baasjaamad on kasutaja ning sensorvõrgu vaheliseks liideseks ning on reeglina ühendatud palju suuremasse ning väiksemate ressursipiirangutega võrku. Üldiselt loetakse baasjaamu usaldusväärseteks, kuigi on mõistetav, et ka baasjaamad võivad saada kompromiteeritud. Peale baasjaamade puuduvad muud usaldusnõuded sensorsõlmede jaoks, kuna nad on haavatavad füüsilistele ja muud tüüpi rünnetele.

Turvalisuse eesmärgid

Turvaeesmärgid sensorvõrkudes sarnanevad paljuski turvanõuetele sardsüsteemides ning on lühidalt kokkuvõetavad järgnevalt:

- **Andmete konfidentsiaalsus**: paljudes rakendustes koguvad sensorvõrgud sensitiivset informatsiooni nagu näiteks meditsiinis või sõjanduses. Andmete konfidentsiaalsus tagab, et andmed on kaitstud ning ei leki väljapoole sensorvõrku volitamatutele osapooltele. Andmete konfidentsiaalsust saab tagada krüptograafiliste meetoditega.
- **Andmete autentimine**: see nõue lubab andmete vastuvõtjal veenduda (kontrollida), et andmed ka reaalselt pärinevad sellelt kübemelt, kust need väidetavalt tulevad. Andmete autentimist aitab teostada sõnumite autentimiskoodid (MAC) kommunikatsioonikanalis.
- **Andmete terviklikkus**: see tagab selle, et andmeid ei ole transpordi ajal muudetud autoriseerimata osapoolte poolt. Üheks andmete terviklikkuse tagamise viisiks on kasutada ühesuunalisi räsimeetodeid enne krüpteerimist.

- **Andmete värskus ja käideldavus**: eeldades, et senorvõrk jälgib ajatundlikke sündmusi, on tähtis tagada võrgust tulevate andmete värskus ja kättesaadavus. See tähendab, et ründaja ei saa vanu sõnumeid tulevikus uuesti saata (ingl k *replay attack*).
- **Sujuv degradeerumine**: see ei pruugi olla küll üks tüüpiline turvanõue, kuid sõltuvalt sensorvõrgu rakendusest võib olla vajalik tagada, et loodud mehanismid oleksid jätkusuutlikud võrgusõlmede kompromiteerimise suhtes. See tähendab, et võrgu jõudlus väheneb sujuvalt, kui osa võrgusõlmi on kompromiteeritud.

Füüsilise kihi ründed

Siin peatükis käsitlen põgusalt meetodeid, mis on võimalikud arupuru kübeme raadiokommunikatsiooni füüsilise kihi ründamiseks ja kaitsemiseks.

Raadikommunikatsoon

Kuigi sensorvõrke võib turvata tavapäraste krüptograafiliste turvameetmetega, et takistada pakettide süstimist või võltsimist, jäävad sensorvõrgud alati haavatavaks rünnetele, mille eesmärgiks on juhtmevaba meediumi kasutamise takistamine. Juhtmevabad sensorvõrgud sõltuvad oma suhtlustasandil täielikul määral vabaleviga raadioeetrist. See aga teeb vaenlase elu väga lihtsaks, võimaldades tekitada raadiohäiretega ründeid, mis üsnagi efektiivselt põhjustavad signaali transmissiooni või vastuvõtu funktsionaalsuses teenusetõkestuse. Teatavasti kui kaks raadioseadet saadavad ühel ajal samal raadiokanalil ning vastuvõtja kuuleb mõlemat, siis vastuvõtja jaoks need signaalid häirivad üksteist. Muidugi sõltub interferentsi mõju sellest, kui tugevad on mõlemad signaalid vastuvõtja pool. Juhul kui üks signaal on märgatavalt tugevam, siis on võimalik üks signaal edukalt kätte saada, kuid võrdse tugevuse puhul ei ole.

Raadiohäired

Raadiohäirimine kasutab ära juhtmevaba meediumi jagatud olemust, takistades seadmete omavahelist suhtelmist. Kui saatja ei saa enam saata või vastuvõtja ei kuule saatjat suure müra tõttu, siis ongi vastava võrgusõlme töö häiritud ning ründaja edukas.

Tulenevalt maksumuslikest piirangutest kasutavad ZigBee standardile vastavad seadmed (ja ka 802.11) liikluse tuvastamise meetodit ühispöörduseks. Liikluse tuvastamise kasutamine meediumipöörduse juhtimises (ingl k *Medium Access Control - MAC*) teeb sensorvõrgud haavatavaks raadiohäiretele, sest vaenlane saab lihtsalt eirata MAC protokolli ning saata segavat signaali teatud kanalil. Selline tegevus takistab MAC protokolli tööd, tekitab pakettide kollisioone või lihtsalt segab transmissioone ümberkaudses sensorvõrgus. Sellepärast on raadiohäire levipiirkonnas olevad sõlmed täielikult isoleeritud kuni vastava raadiohäire lõppemiseni.

Raadiohäire rünnakul on mitmeid erinevaid strateegiaid. Järgnevalt toon välja neli põhilist ründeviisi, millest kolm esimest on aktiivsed ründed ning viimane reaktiivne.

Pidev häirija

Pidev häirija saadab kogu aeg raadiosignaali, mida võib teha mingi singaaligeneraatoriga või tavalise raadioseadmega, saates juhuslikku bitijada ning eirates MAC etiketti. Kuna MAC protokoll lubab legitiimsetel kübemetel saata ainult siis, kui võrk on jõude, takistab pidev segaja kübemetel kanali üle kontrolli saamast. Tegu on kõige lihtsama, kuid samas väga energiakuluka ründeviisiga.

Kurnav häirija

Selle asemel, et saata pidevalt välja suvalist bitijada, saadab kurnav häirija pidevalt normaalse struktuuriga pakette, ilma et ühegi paketi vahele jääks tühja auku. Lõpptulemusena on normaalsed kübemed petetud, arvates, et pidevalt saadetakse legitiimseid pakette, ning on sunnitud olema vastuvõtu olekus. TinyOS-i (kübemetel kõige laialdasemalt kasutatav operatsioonisüsteem) puhul on paketi preambula vastuvõtmisest alates kübe sunnitud vastuvõtu olekusse, olenemata, kas kübemel endal on midagi saata või mitte.

Juhuslik häirija

Selline häirija ei saada raadiosignaali pidevalt, vaid vaheldumisi magab ja siis saadab. Peale mõnda aega segava signaali saatmist lülitab ta raadio välja ning läheb puhkerežiimi ning mõne aja pärast kordab häiresignaali saatmist. Saatmise faasis võib ta käituda kui pidev häirija või siis kui segadust külvav häirija. Juhuslik häirija üritab arvestada energiasäästuga, mis on eriti tähtis segajatel, millel pole piiramatus mahus toidet.

Reaktiivne häirija

Eelneva kolme ründetüübi korral oli tegu aktiivse ründega, selles mõttes, et rünnati kommunikatsioonikanalit olenemata seal toimuvast liiklusest. Aktiivründed on efektiivsed, kuna hoiavad kanalit kogu aeg hõivatuna, kuid selliseid ründeid on ka kõige kergem tuvastada. Alternatiivset lähenemist pakub reaktiivne häirija, kes on vait kuni kanal on jõude ja hakkab saatma siis, kui ta tunnetab kanalil aktiivsust. Sellist ründajat on juba raskem tuvastada.

Raadiohäire ründe eeliseks on tema lihtsus – pole vaja mingit tarkust rünnatava sensorvõrgu kohta, tuleb ainult teada kübemete suhtluskanalit. Sellise ründe nõrgaks küljeks on suur energiatarve, mis kaasneb pideva või liigse häiresignaali saatmisega, põhjustades ründaja kiire energiavarude vähenemise.

Füüsiline vigastamine

Füüsilise kihi ründe alla kuulub ka kübeme füüsiline vigastamine, näiteks raadio hävitamine. Samuti võib füüsiliselt kübemele juurdepääsu saanud ründaja seadmest kasulikku infot välja võtta, nagu näiteks turvavõtmed võrgu kõrgematele kommunikatsioonikihtidele ligi pääsemiseks.

Rünnete tuvastamine

Rünnete tuvastamine on tähtis, kuna see on esimene samm ehitamaks turvalist ning usaldusväärset juhtmevaba võrku. Raadiointerferents rünnete tuvastamise teeb keerukamaks asjaolu, et on vaja eristada legitiimseid ja ründaja poolt tekitatud kehva ühenduvuse põhjuseid. Just võrgu ülekoormusest ja seadmete tõrgetest tulenevad stsenaariumid on eriti raskesti eristatavad raadiohäire rünnetest. Ründe tuvastamiseks saab kasutada mitmeid erinevaid võrgu parameetreid nagu näiteks signaalitugevus, võrguhõivatuse aeg või pakettide kohaletoimetamise määr.

RSSI

Vastuvõetud signaalitugevuse hindamine (ingl k *Received Signal Strengrh Indication - RSSI*) ja selle võrdlemine mingi konstantse lävega (nagu seda tehakse MAC protokollis) või siis adaptiivse lävega (BMAC protokollis) ei ole üksinda abiks, kuna pole võimalik eristada normaalset paketi saatmise läve häire lävest. Samuti ei aita normaalse RSSI signaalikuju võrdlemine ründe omaga, sest sellisel juhul ei oleks eristatavad normaalne saatmine ja reaktiivse segaja häired.

Võrguhõivatuse aeg

Kuna segaja võib legitiimsel kübemel takistada pakettide väljasaatmist, sest kanal tundub pidevalt olevat hõivatud, siis võrguhõivatuse aeg võib tunduda üsnagi mõistliku parameetrina ründaja tuvastamiseks. Tuleb välja, et seda parameetrit annab kasutada ründe tuvastamiseks kui on täidetud järgnevad kaks tingimust: esiteks ründaja ei ole reaktiivne ega ka juhuslik ja MAC protokoll kasutab kanali jõude oleku tuvastuseks fikseeritud lävendit. Sellisel juhul saab eristada häire stsenaariumit võrgu ummistumise stsenaariumist, sest viimase korral on võrguhõivatuse aeg tõkestatud, kuigi võib olla pikk, ründe korral aga tõkestamata.

Pakettide kohaletoimetamismäär

Pakettide kohaletoimetamismäär (ingl k *Packet Delivery Rate - PDR*) aitab samuti tuvastada häirija olemasolu, kuna ründe korral läheneb PDR väärtus nullile. Et teada saada PDR määr, kust alates võib tegu olla ründaja poolt tekitatud raadiohäiretega, on tarvis teada võrgu enda dünaamika (ülekoormuse) poolt põhjustatud kanalikvaliteedi langust. Nagu selgub artiklist [3], siis maksimaalse koormuse korral jääb PDR väärtus 78 protsendi piirimaile. Seega saab lihtsa lävendi mehhanismiga eristada raadiohäireid võrgu enda ülekoormusest ning seda olenemata ründe strateegiast. PDR ei aita tuvastada selliseid olukordi, kus saatja liigub kommunikatsiooni ulatusest välja või saatja toiteallikas saab tühjaks. Samas oma dünaamikalt on need olukorrad üsna sarnased ründe olemusega, sest PDR väärtus langeb analoogselt.

Kuna eelpool mainitud meetodid üksi ei ole piisavalt adekvaatsed, et alati tuvastada ründeid, siis on mõttekam kasutada nende kombinatsiooni. Näiteks PDR koos signaalitugevusega. Nimelt saab teha mõõtmised normaalolukorras ning selgitada välja seosed PDR ja signaalitugevuse vahel ning siis rakendada seda teadmist ründe korral, eristamaks ründeolukordi normaalsest [4].

Kaitsemeetodid

Tulenevalt füüsilise kihi rünnete iseloomust on kaitsemeetodite osas mõttekas lähtuda Sun Tze kuulsast *The Art Of War*-st: „*He who cannot defeat his enemy should retreat*“. Ehk tõlgendades seda filosoofiat juhtmevaba kommunikatsiooni maailma: kui puuduvad piisavalt võimsad saatjad, et segajatest üle rääkida, siis on taganemisteedeks spektraalne või ruumiline taganemine.

Spektraalne taganemine

Spektraalne taganemine hõlmab endas kanalivahetust. Kuna segaja on reeglina kindlal kanalil, siis on targem vahetada suhtluskanal mõne teise vastu, kus segajaid ei ole. Kuna raadiohäiretega keskkonnas pole võimalik teistele osapooltele öelda, mis kanalile minna, siis on tarvilik määrata kanalivahetuse algoritm. Siin on võimalik kaks skeemi: koordineeritud kanalivahetus või spektraalne multipleksimine. Esimesel juhul terve võrk vahetab kanalit, mis aga suure võrgu puhul põhjustab märgatavat latentsust. Teisel juhul ainult raadiohäire piirkonnas olevad kübemed vahetavad kanalit ning häire piirimail olevad kübemed täidavad multiplekseri ülesannet erinevate spektraaltsoonide vahel. See töötab eeldusel, et ründaja ei tea kanalivahetuse järjekorda.

Ruumiline taganemine

Ruumiline taganemine tuleb kõne alla ainult mobiilsete võrgusõlmede korral ning eesmärgiks on liikuda ründaja häiresignaali ulatusest välja. Kokkuvõtlikult on selle strateegia puhul kaks faasi: esiteks põgenemise faas, kus liigutakse ohutusse tsooni, ning teiseks võrgu rekonstrueerimisfaas, mille käigus ehitatakse võrk jälle üles.

Üle karjumine

Üheks võimaluseks on tõesti ka raadio saatevõimsuse tõstmine, et rääkida häiresignaali tekitajast kõvemini, parandades signaali-müra suhet. Kuid see toob endaga kaasa suurenenud energiakulu ning samas võib ründaja kasutada täpselt sama taktikat. Lisaks tuleb arvestada, et suurendatud saatevõimsusega kaasneb ka leviulatuse kasv ning sedasi võidakse häirima hakata kaugemal olevate kübemete omavahelist kommunikatsiooni.

Hajaspektermodulatsioon

Telekommunikatsiooni valdkond tunneb ka ülilairiba meetodit (ingl k *Ultra Wide-Band – UWB*), mida on peaaegu võimatu raadiohäiresignaalidega segada. UWB põhineb väga lühikeste (nanosekundite pikkuste) pulsside saatmises suures sagedusvahemikus üheaegselt. Kuna UWB-l on üsna väike energiatarve, siis peaks see juhtmevabadele sesnorvõrkudele sobima ideaalselt, kuid see eeldab vastava raudvara olemasolu [5]. Kui aga ründajal peaks olema piisavalt suure sagedusulatusega segaja, mis katab ära 802.15.4 standardi sagedusala, siis ei aita ka UWB.

Vandalismikindel disain

Esiteks tuleks kübemed maskeerida ning paigutada nii, et neid oleks raske leida. Teiseks tuleks korpus teha võimalikult vandalismikindlaks. Kui võimalik, siis peaks kübe füüsilisele ründele reageerima *fail-complete* viisil, kustutades programmimälu või vähemalt sensitiivse info nagu krüpteerimisvõtmed.

Kanalikihi ründed

Antud peatükis võtan lühidalt kokku võimalikud ründed ja kaitsemeetodid raadiokommunikatsiooni andmelülikihil, mis võimaldab suhtlust naabervõrgusõlmedega.

Kollisioonid

Põrkeründe korral kasutab vaenlanen oma raadioseadet, et kuulata WSN töökanalil ning kui ta tuvastab sõnumi väljasaatmist, saadab ka ise signaali välja, mis segab legitiimset transmissiooni. Eri signaalide samaaegset edastust ühes kanalis tekitab põrke (kollisiooni). Teoreetiliselt piisab vaid ühe sõnumibaidi ulatuses põrke tekitamisest, et rikkuda sõnum ning tekitada tsükkelkoodkontrollis (ingl k *Cyclic Redundancy Check – CRC*) ebakõla. Kui paketi pealt arvutatud kontrollsumma ei lange kokku saadetud kontrollsummaga, siis TinyOS ignoreerib seda paketti. Tähele tuleb panna seda, et preambula rikkumine ei tekita CRC ebakõla, kuna seda ei arvestata kontrollsumma arvutamisel. Kontrollsummas ebakõla tekitamiseks piisab paketi päise rikkumisest, kuid kindlam oleks rikkuda paketi kasuliku lasti osa, sest TinyOS versioon 1.x ei ignoreeri vigast paketti ning sedasi võib ikkagi paketi rikkumata lasti kätte saada.

Põrkeründe eelis raadiohäire tekitamisründe ees on energiatarve. Põrkeründe korral ollakse saaterežiimis väga lühikest aega, sest piisab põrkest ühe-kahe baidi ulatuses, et terve pakett oleks rikutud. Erinevus reaktiivse häirijaga on see, et reaktiivne häirija saadab segavat signaali terve paketi sõnumi sisu saatmise ajal. Seega on põrkerünnet sama raske ära tunda kui reaktiivset rünnet.

Kaitsemeetodid

Põrkeründe vastu aitavad kõik samad vastuabinõud ja tuvastusmeetodid, mis füüsilise kihi rünnete juures. Lisaks võib siinjuures aidata ka veaparanduskoodide kasutamine, teatud piiratud arvu baitide parandamiseks. Kui ründaja teab seda, saab ta alati tekitada kollisioone rohkemas arvus baitides ning siis pole vastavatest koodidest enam kasu. Kui paketistruktuur on ründaja jaoks teada, siis saab palju

efektiivsema põrkeründe teha, rünnates paketi pikkuse baiti. See põhjustab protokollil vale arvu baitide vastuvõtu ning veatuvastus ning veaparanduskoodidest ei ole enam mingit abi.

TinySec

Üheks võimaluseks, kuida kaitsta võrgukihi kaudu saadetud sõnumeid on nende krüpteerimine kanalikihis, mida TinyOS-i jaoks pakub TinySec [6]. TinySec on kanalikihi turvaprotokoll, mis tagab pääsu reguleerimise (ingl k *access control*), sõnumi terviklikkuse (ingl k *message integrity*) ja sõnumi konfidentsiaalsuse (ingl k *message confidentiality*). Pääsu reguleerimisega tagatakse võrgus osalemine ainult autoriseeritud osapooltele ehk legitiimsed võrgusõlmed suudavad tuvastada volitamata võrgusõlme sõnumid ning eiravad neid. Sõnumi terviklikkus tähendab, et sõnumi saatmise ajal ei ole seda mõni teine osapool muutnud ning see on tagatud sõnumi autentimiskoodiga (ingl k *Message Authentication Code – MAC*). Sõnumite krüpteerimiseks kasutab TinySec Skipjack-i [7], mis kasutab 80-bitist võtit. Kuigi on teada ründeid Skipjack algoritmi mõnedele osadele [8], siis ei eksisteeri rünnet algoritmi kõikidele osadele ning sellepärast ei ole ka reaalne leida mõistliku aja jooksul võtit kasutades isegi superarvutit, rääkimata piiratud ressurssidega kübemest. Eksperimendid on näidanud, et lisakulud – energiakulu, latentsuse ja ribalaiuse tõus –, mida TinySec kasutamine kaasta toob, jäävad alla 10%.

Võrgukihi ründed

Selles peatükis uurin võimalikke ründeid ja kaitsemeetmeid kommunikatsioonimudeli võrgukihis, kus ründe alla satuvad ruutimisprotokollid ehk loogilise võrgu toimimise alustalad.

Marsruutimine

Ruutimisprotokolli ülesanne arvutivõrgus on leida teekond lähtepunktist sihtpunktini, lubades neil osapooltel vahetada informatsiooni mööda vastavat teed. Enamus marsruutimisprotokolle otsivad parimat teed lähtuvalt teatud maksumusest ja meetrikast nagu hüpete arv, minimaalne energiakulu, lühim tee jne. Juhtmevabas sensorvõrgus tekivad sellised rajad reeglina baaskübeme juurde, moodustades täispuu (ingl k *spanning tree*).

On olemas kaks põhilist ruutimistehnoloogiat: kanalioleku (ingl k *link state routing*) ja kaugusvektori (ingl k *distance vector*) põhjal marsruutimine. Kanalioleku ruutimisprotokoll teab kogu võrgu struktuuri ja ühendusi eri sõlmede vahel. Iga sõlm arvutab iga võimaliku sihtkoha jaoks parima järgmise sihtkoha ning annab sellest teada teistele. Antud protokolli puuduseks WSN-s on selle suurem mälu- ning arvutusnõudlus kui kaugusvektori protokolli korral. Kaugusvektori protokolli korral omatakse ruutimistabelit ainult naabersõlmede kohta ning nendega vahetatakse ka ruutimisinfot, mis teeb nõuded mälule ja arvutusmahule hulga väiksemaks.

Ruutimisprotokollide vastu eksisteerivad mitmed erinevad ründetüübid, millest kõige levinumad on selektiivne edastus (ingl k *selective forwarding*) [11], *sinkhole*, HELLO uputus (ingl k *HELLO flood*), ruutimistsüklid (ingl k *routing cycles*) ning identiteedi rünne (ingl k *Sybil attack*) [9]. Järgnevalt seletan lühidalt lahti nende rünnete olemused ning siis vaatan mõningate enamlevinud ruutimisprotokollide näol nende rünnete realiseeritavust.

Selektiivne edastus

Selektiivedastusründe korral saadab võrgusõlm edasi enamus sõnumeid ning selektiivselt eirab üksikuid sõnumeid, mida ta edasi ei saada. Selektiivset edastust võib kombineerida teiste ründetüüpidega, mis tõmbavad endaga kaasa võrguliiklust nagu näiteks *sinkhole*.

Sinkhole

Sinkhole ründe korral üritab vastav võrgusõlm endale tõmmata nii palju võrguliiklust kui võimalik ümberkaudsest võrgust. See saavutatakse tavaliselt tehes endast väga atratkiivse sihtpunkti lähtuvalt ruutimismeetrikast või teeseldes baasjaamaks olemist. Sellisel juhul üritavad ümberkaudsed võrgusõlmed kogu liikluse suunata just *sinkhole* sõlmele, mis annab talle väga suure mõjuvõimu terves sensorvõrgus.

HELLO uputus

HELLO uputuse korral kasutab ründaja hästi võimast raadiosaatjat, et saata sõnumeid tervele (või suuremale osale) võrgule. Sõnumite eesmärgiks on veenda kõiki võrgusõlmi valimaks ründaja, kes tõenäoliselt on nende kuuldeulatusest väljas, nende järgmiseks sõnumi edastuse sihtpunktiks.

Ruutimistsüklid

Kui esineb ruutimistsükkel, siis teekond lähtepunktist sihtpunkti omab endas tsüklit, mis tähendab, et sõnum jääda lõputult ringlema, põhjustades lõpuks kübemete toiteallika tühjenemise.

Identiteedi rünne

Sybil rünne, mille korral omab üks võrgusõlm mitut erinevat identiteeti ning kasutab neid, et täita naabervõrgusõlmede mälu kasutute andmetega olematute võrgusõlmede kohta. Kui võrgusõlmede ruutimistabelite maht on piiratud, võib sedasi kasulikud andmed lasta üle kirjutada.

Multihop

Multihop ruutimisalgoritm on üks lihtsamaid ja levinuimad TinyOS-i keskkonnas. Algoritm valib eelisjärjekorras lühima tee ehk kõige väiksema hüpeta arvuga raja. Lisaks arvestatakse iga sõlme kohta vastuvõtu ja saatmise kvaliteedi hinnangut.

Selektiivedastuse rünnet on multihop võrgus väga lihtne korraldada. Nimelt kui võrgusõlm käitub enamus ajast lihtsalt järgurina (ingl k *repeater*), mis ei arvesta ennast hüpete arvu sisse, siis tundub kõrvalolevatele sõlmedele, et läbi järguri on teekond sihtkohta lühem ning nad hakkavadki temale pakette edastama. Ründe efektiivsus sõltub järguri paigutusest võrgus, mida lähemal baasile, seda suurema võrguliikluse saab ta omale tõmmata; ning kõrvaldatud sõnumite osakaalust. Kui järgur kõrvaldaks liiga palju pakette, siis tema lingi kvaliteet teiste silmis alaneks ning lõpuks ei edastataks talle enam üldse pakette. Tuleb välja, et kui kõrvaldada alla 35% pakettidest, siis ei muutu tema kvaliteet nii halvaks, et teised sõlmed peaksid hakkama kaaluma teist rada, samas juba üle 65% korral ei edastataks talle üldse pakette.

Kui omatakse pisut rohkem teavet ruutimisalgoritmi kohta, siis on juba mõttekam sekkuda ruutimismehanismi ning luua *sinkhole*. Lihtsaimal juhul tuleb kuritahtlikul kübemel teeselda vaid baasjaama, mis võib põhjustada suure osa võrguliikluse suunamist juba *sinkhole*-le. Mõjutatud võrgusõlmede arv sõltub *sinkhole*-i paigutusest võrgu struktuuris – õigele baasjaamale lähemal olevad kübemed ei hakka saatma pakette *sinkhole*-le, kuid kaugemal olevad võivad küll. Multihop võrgus saadavad võrgusõlmed oma naabritele perioodiliselt välja teekonna uuendusi. Sõnum sisaldab sõlme ID-d, hüpete arvu baasini ja iga naabri kohta lingi kvaliteediinfot. Kui sõlm valib omale järgmist

hüpet, siis jätab ta valikust välja alla 25%-lise kvaliteediga sõlmed, samas nullise hüppe korral ei arvestata kvaliteeti üldse. Selliseid uuendussõnumeid saab *sinkhole* ära kasutada oma hüvanguks, saates sõlmedele, kes temale sõnumeid ei edasta väära sisuga uuendusteateid. Kuid Multihopil on veel üks sptetsiifilisem mehanism, mida saab ära kasutada. Nimelt iga sõlm nummerdab sõnumeid, mida ta välja saadab. Vastuvõtja sõlm kontrollib seda numbrit ning teeb vastavalt sellele lingi kvaliteedi arvutusi, kui aga järjekorra number on üle 20 väiksem eelmisest, siis vastuvõtja sõlm nullib tabelis lingi kvaliteedi näitajad sõlme kohta, kust see sõnum tuli. Nüüd piisab kui kuritahtlik kübe saadab kaks sõnumit, mis paistavad tulevat mingilt kolmandalt sõlmelt ning teise sõnumi järjekorra number on 20 võrra väiksem eelmisest, et teeseldud võrgusõlme lingi kvaliteet ära nullida sõlmes, kuhu teated saadeti.

Lühima tee eelistamist saab ära kasutada HELLO uputusründega. Sellisel juhul saadab kuritahtlik kübe võimsa antenniga kõigile võrgus olevatele sõlmedele teate, et tema on baasjaam, mistõttu peaksid vastuvõtjad võrgusõlmed otsustama, et lühim tee on läbi HELLO uputust teinud võrgusõlme ja hakkavad temale pakette edastama, kuigi ta ei pruugi olla üldse nende kuuldeulatuses. Ainsaks miinuseks on see, et õige baasjaam saadab aegajalt sarnast tüüpi sõnumeid, sellepärast tuleb iga teatud aja tagant sõnumit korrata. Üldiselt on HELLO uputus üsna energiakulukas ründetüüp.

Multihop sisaldab hüpeta arvu loendurit, kui palju hüppeid on sihtkohani veel jäänud. Iga võrgusõlm, kust sõnum läbi läheb vähendab seda loendurit ning sellepärast ei ole ruutimistsüklid Multihop võrgus võimalikud. Loenduri nulli jõudmisel heidetakse sõnum minema, kuna see võib tähendada tsükli olemasolu.

Multihop protokoll hoiab infot naabrite kohta vastavas tabelis, mille suuruseks on 16 sissekannet, siis on täiesti võimalik *Sybil* ründega kogu mälu kasutu infoga täita. Kui kübe saab teate uuest naabrist ning tabel on täis, siis asendatakse kõige väiksema saatekvaliteediga naabri kirje. Seega kui *Sybil* rünnet tegev sõlm võtab endale 16 erinevat identiteeti, siis võimalik kõik legitiimsed naabrid mälust kõrvaldada. Ründe nõrgaks küljeks on suur sõnumite arv, mis on tarvis saata.

Mintroute

Mintroute marsruutimisalgoritm on mugandatud Multihop. Ainus erinevus seisneb vanemsõlme valimise algoritmis. Kui Multihopis kasutatakse väikseimat hüpete arvu, siis Mintrouti korral arvestatakse ümbritsevate naabrite kvaliteedinäitajaid koos kumulatiivse teekonna hinnanguga baasjaama. Hüpete arvu ignoreeritakse täiesti. See tekitab ühe nõrga külje, nimelt kui eksisteerib kaks võrdse kõrgeima kvaliteediga naabrit, siis Mintroute teeb valiku suvaliselt ning sedasi võib osutuda valituks baasist kaugemal asuv kübe. Tulenevalt Mintroute suurest sarnasusest Multihopile, käsitlen ründeid pisut lühemalt ning toon välja ainult suuremad erinevused.

Selektiivedastusrünne ei ole Mintrouti korral nii efektiivne, sest siin ei anna lühem tee mingit eelist – loeb ainult lingi kvaliteet. Kui kuritahtlik võrgusõlm kõrvaldab pakette, siis tema lingi kvaliteet teiste silmis väheneb ning teda püütakse vältida. Kuna Mintrouti korral iga lisa võrgusõlm, mida pakett peab läbima vähendab lingi kvaliteeti, siis ei tundu selektiivedastaja sõlm nii ahvatlev.

Samuti ei ole *sinkhole* rünne nii lihtne kui Multihopi korral. Võrgusõlme naabriks võib olla baasjaam, kuid paljalt selle otsuse järgi ei valita omale vanem-võrgusõlme, otsus langetakse ikkagi parima lingikvaliteedi alusel. Seega lihtsalt baasi teesklemisest ei piisa, et kogu võrguliiklust endale meelitada. Et osutuda valituks peab *sinkhole* omama head saatmise ja vastuvõtu kvaliteeti ning selle

saamiseks peab ta piisavalt pakette edastama. *Sinkhole* saab ära kasutada Multihopist teada sõnumi järjekorra numbri petuskeemi, et teiste sõlmede kvaliteeti nullida.

Ülejäänud ründetüübid ei oma Mintrouti korral mingeid erinevusi. Ainult HELLO uputusründe korral peab vastav võrgusõlm oma saadetud sõnumite määra kõrgel hoidma, et säilitada oma kõrge vastuvõtu kvaliteet.

DSDV

DSDV (Destination-Sequenced Distance Vector) on kaugusvektoril põhinev ruutimisprotokoll, mis pakub mitu-ühele marsruutimist kas hüpete arvu või kvaliteedi meetrika järgi. DSDV korral saadab baasjaam perioodiliselt välja teate enda ID-ga, meetrikaga ning teate järjekorranumbriga. Kõik sõlmed, kes kuulevad seda sõnumit edastavad selle ning kasutavad vastavat ID enda sihtkohana. Sedasi luuakse iga taolise teatega võrgus täispuu.

Hüpete arvu meetrika

Selle meetrika korral kasutatakse sihtpunktini teekonna valimisel minimaalset hüpete arvu. See on väga sarnane Multihopile, kuid puudub lingi kvaliteedi parameeter. Kokkuvõttes vahetatakse vanemsõlm välja ainult juhul, kui leitakse lühem tee.

Selektiivedastus töötab pareminigi kui Multihopi korral, kuna ainukeseks parameetriks, mida jälgitakse on hüpete arv sihtkohta. Kuritahtliku kübeme ainsaks ülesandeks on edastada piisavalt teekonna uuendussõnumeid, et teised kübemed ei vahetaks välja enda vanem-võrgusõlme, kõik muud sõnumid võib aga puhta südamega kõrvaldada.

Sinkhole ründe korral on mitu lähenemist. Esiteks võib võrgusõlm teeselda baasjaamak olemist ning saata välja teavitussõnumeid enda ID-ga, mis mõjutab kõiki võrgusõlmi endale sihtkohaks valima *sinkhole* ID-d ning leidma sinna lühimat teed. Selline struktuur kehtib kuni õige baasjaam saadab välja oma teavituse, peale mida kõik võrgusõlmed muudavad oma sihtkoha jälle õigeks. Teiseks võimaluseks on teeselda lühima tee omamist õigesse baasjaama. See mõjutab kõiki võrgusõlmi, mis on *sinkhole*-ile lähemal kui õigele baasjaamale, oma liiklust suunama just *sinkhole*-i. Kuna võrgusõlmed ei muuda sihtkoha ID-d, siis ei muuda nad ka oma teekonda, isegi peale õige baasjaama uut teadet. DSDV kasutab sõnumite järjekorra märkimiseks järjekorra numbreid, selle numbri alusel praagitakse välja ka vanad ning duplikaatsõnumid ja saadakse teada vahelejäänud sõnumite kohta. Kui sõnumi number on vähem kui 64 võrra väiksem kui eelmine, siis on tegu vana sõnumiga ning seda eiratakse. *Sinkhole* saab kopeerida legitiimse baasjaama teadet ning suurendades vähemalt 4 võrra järjekorra numbrit saab sundida kõiki võrgusõlmi endale uut vanemat valima, sest kõik arvada, et nad on maha maganud vähemalt kolm uuendusteadet ning sedasi valitakse teekond *sinkhole*-i juurde. Kui *sinkhole* hoiab järjenumbrit kuni 64 võrra suuremana õige baasjaama järjenumbrist, siis ei reageeri võrgusõlmed õige baasjaama teavitussõnumitele. Kokkuvõttes peab *sinkhole* saatma ühe teavitussõnumi (suurendades järjenumbrit 64 võrra) 64 legitiimse baasjaama teavitussõnumi kohta, et hoida võrguliiklust endale suunatud.

HELLO uputuse korral on valida samade võimaluste vahel nagu *sinkhole* ründe korral. HELLO uputus sõlm või teeselda teist baasjaama uue ID-ga või, mis on palju efektiivsem, teeselda reaalset baasjaama. Sel juhul valivad sõlmed reaalse või võltsbaasjaama, mis on neile kõige lähemal. Seega kui HELLO võrgusõlme sõnumit kuulevad kõik võrgu sõlmed, siis valitakse tema järgmiseks hüppeks, kuigi

ta võib paljude jaoks olla levist väljas. Selline halvatud olukord valitseb võrgus seni kuni HELLO sõlm jätkab teekonna sõnumite levitamist.

Kuna DSDV ei oma mingit kaitset tsüklite kohta, siis võib selle ruutimisalgoritmi korral tekitada väga kergesti võltsitud ruutimisteadete kaudu kinniseid ringe, kus sõnumid jäävadki ringlema, kuni kübemete toide otsa lõpeb.

Kvaliteedi meetrika

Kvaliteedimeetrika kasutamise korral DSDV-s kaasab võrgusõlm ruutimisteatesse endale teada oleva ruutimisteekonna kvaliteedi. Üldiselt kõik sõlmed hoiavad end kursis kõigi enda naabrite linkide kvaliteetidega. Kvaliteet on määratud viimasest 32-st sõnumist kättesaamata jäänud sõnumite arvuga. Saades ruutimisuuenduse teate võtab võrgusõlm vastava naabri lingi kvaliteedi ning liidab sinna otsa sõnumis oleva kvaliteedi näitaja ning valib kõige väiksema summaga sõlme enda vanemaks.

Selektiivedastusrünne ei tööta antud juhul nii hästi kui hüpete meetrika korral, sest iga lisa hüpe toob endaga kaasa lingi kvaliteedi halvenemise ning kui selektiivedastus võrgusõlm kõrvaldab liiklusest veel sõnumeid ka, siis on lingikvaliteet läbi selle sõlme veel kehvem ning tõenäoliselt ei osutu see üldse valituks.

Kvaliteedimeetrika kasutamine ei avalda *sinkhole* ründe efektiivsusele mingit mõju võrreldes hüpete arvu meetrikaga. Niisamuti töötavad ka HELLO uputus ja ruutimistsüklite ründed.

TinyAODV

TinyAODV on lihtsustatud versioon nõudmisel põhineva ad hoc vektor marsruutimisprotokollist. Tegu on nõudmisel põhineva ruutimisalgoritmiga, mis tähendab, et rada lähtepunktist sihtpunkti luuakse siis kui vaja. Kui üks sõlm tahab saata sõnumit teise, siis edastab ta teekonna soovi päringu. Kui sihtkoht seda kuuleb, siis saadab ta välja teekonna vastuse, mis liigub tagurpidi tuldud teed tagasi. Kõik sõlmed, mis jäävad selle tee peale salvestavad omale antud tee ruutimistabelisse, kus on ruumi seitsmele sissekandele. Teekonnad ei aegu kunagi, aga tabeli täitudes vanemad sissekanded asendatakse. Teekonnad seatakse üles lihtsa vähem hüpete meetrika alusel.

Selektiivedastusrünne töötab täpselt samamoodi nagu DSDV hüpete meetrika korral, ainukeseks erinevuseks on see TinyAODV korral võib lähte ja sihtpunkt asuda ükskõik kus võrgu punktis ning seega on tähtis selektiivedastusründe korraldaja paiknemine lähte ja sihtpunkti suhtes.

Kuna TinyAODV korral pole ühte kindlat baasjaama vaid iga sõlm võib olla sihtpunktiks, siis *sinkhole*-i ei saa nii kergesti imiteerida ühte sõlme ja meelitada kogu võrguliiklust omale. Et oma mõjuulatust maksimeerida tuleks *sinkhole*-l iga teekonna koostamisest osa võtta ning niipea kui ta kuuleb päringut mõne teekonna kohta peaks ta vastama, et on selle leidnud vähima arvu hüpetega ning saatma vastuse. Ning kõik sõlmed, mis jäävad teekonnale salvestavad omale ruutimistabelisse vastava teekonna *sinkhole*-i. Kui aga reaalne sihtkoht on lähemal kui *sinkhole*, siis valitakse ikka õige sihtkoht.

HELLO uputus ründe korral saaks *sinkhole* saata vastuse otse lähtepunktile ning kuna lähtepunktile tundub sihtkoht vaid ühe hüppe kaugusel, siis valibki ta *sinkhole* otse sihtpunktiks. Niimoodi saab väga kergesti terve võrgu ära halvata.

Ka ruutimistsüklit on võimalik tekitada, selleks kulub kuritahtlikul sõlmel kolme sõnumi saatmisest, et halvata kahe võrgusõlme töö.

Transpordi kihi ründed

Transpordi kiht haldab otspunktide vahelisi ühendusi. Transpordikiht võib pakkuda hästi lihtsat teenust nagu ebausaldusväärset suvaedastust või usaldusväärset järjestatud multiedastust. Siin peatükis vaatan võimalikke ründed transpordi kihi teenustele.

Üleujutamine

Protokollid, mis peavad säilitama olekut mõlemas kommunikatsiooniahela otsas on haavatavad mälu õgimise osas üleujutamise kaudu. Nagu klassikalises TCP SYN üleuputamises saadab vaenlane palju ühenduse loomise päringuid ohvrile. Iga päringu peale üritab ohver eraldada ressursse, et säilitada vastava ühenduse kohta olekuinfot. Lõpuks aga saavad vabad ressursid otsa ning siis enam uusi ühendusi ei saa ohvrile teha.

Kaitsemeetmed

Piirates maksimaalset ühenduste arvu, saab vältida ressursside täielikku ammendumist, mis segaks ohvri kõiki teisi protsesse. Samas see meetod takistab ka teistel legitiimsetel võrgusõlmedel ohvriga ühendust võtmast, kuna mälu on hõivatud võltsühendustega. Kuigi ühendusevabad ning seega olekuvabad protokollid peavad sellele ründele mõnevõrra paremini vastu, ei pruugi nad pakkuda piisavalt adekvaatseid transpordikihi teenuseid.

Üheks kaitsestrateegiaks on kliendi mõistatuste lahendamine [15]. Niimoodi demonstreerivad kliendid oma pühendumust loodavasse ühendusse ning on selle nimel nõus enda ressursse raiskama. Serveri ülesanne on selliseid mõistatusülesandeid levitada ning kontrollida nende õigsust. Sellisel juhul peab ründaja palju rohkem enda arvutusressursse raiskama serveri ründamiseks, et tekitada ühenduste üleujutusi. Kõrge koormuse korral võib server muuta ülesannet veel raskemaks, et potentsiaalsete klientide arvutuskoormust veel tõsta. Muidugi on selline starteegia mõttekas kui vaenlastel on samasugused ressursside piirangud kui tavalistel sõlmedel.

Desünkroniseerimine

Olemasolevat ühendust otspunktide vahel saab segada desünkroniseerimise kaudu [16]. Sellisel juhul saadab ründaja korduvalt võltsitud sõnumeid mõlemale osapoolele. Vastavad sõnumid kannavad endas järjenumbrit või kontroll-lippe, mille tagajärjel hakkavad osapooled kaduma läinud pakette uuesti küsima. Kui ründaja suudab ennast pideval õigesti ajastada, siis saab sedasi takistada ühenduse otspunktidel omavahel mõistlikke sõnumite vahetamist, põhjustades energia raiskamist pidevale sünkroniseerimisele ja pakettide taastamisele.

Vastumeetmed

Vastumeetmeks on kõikide vahetatavate pakettide autentimine. Seal juures peavad olema autenditud ka transpordi protokolli kõik päise väljad. Sellisel juhul, kui ründaja ei oska võltsida autentimismehanismi, tuvastavad osapooled kuritahtlikud paketid ning eiravad neid.

Kokkuvõte

Ründed juhtmevabade sensorvõrkudele on erinevatel võrgukihtidel erinevad, seega tuleb turvalisust silmas pidades lähtuda samuti mitmetasemelisest mudelist. Nagu analüüs näitas, on sensorvõrgud haavatavad kõigil käsitletud kommunikatsioonikihtidel ning turvalise võrgu loomisel on tarvis alustada juba aluskihtidest alates. See tähendab, et raadiohäirete ning kollisioonide vältimiseks peaks tähelepanu pöörama juba raudvara valikus. Näiteks üsna efektiivsed vastumeetmed füüsilise kihi rünnetele on kas sagedushüpped (ingl k *frequency hopping*) või UWB, kuid mõlemad peaksid olema raudvaraliselt toetatud. Samas ründekindel raudvara ei tähenda, et tarkvara turvalisust saaks ignoreerida. Kuna kõigis ruutimisalgoritmides on sees nõrki külgi, siis oleks mõttekas turvalisuse tõstmiseks kasutada krüpteeringut, mida pakub TinySec, juba kanalikihis, mis aitab ära hoida pealtkuulamist, pakettide modifitseerimist ja kordamis. Väljatoodud arutluses on selgelt näha mainitud levinud marsruutimisalgoritmide nõrgad küljed. Fakt on see, et ükski käsitletud ruutimisprotokollidest ei olnud ründekindel, samas nii mõnegi turvariski saaks üsna pisikese algoritmiliste muudatusega kõrvaldada. Saab kasutada ka täiendavaid tarkvaralisi lahendusi. Näiteks identiteedivarguse rünnet (*Sybil attack*) saab takistada kergekaaluliste identiteedi sertifikaatidega, mis kasutavad ühesuunalisi võtmeahelaid ning Merkeli räsipuud [10]. Niisamuti on välja pakutud selektiivse edastuse ründe tuvastamise skeem läbi multi-hop kviteerimistehnika, mis tõstab tuvastustäpsuse 95%-ni [11], selle vastu võib aidata ka näiteks mitmeharuline ruutimine [13, 14].

Üldiselt on aga väga raske, kui mitte võimatu kaitsta sensorvõrku kõigi võimelike rünnete vastu, samas iga sensorvõrk ei vajagi kaitset kõigi võimalike rünnete vastu ning turvalisuse tase peaks olema rakenduse spetsiifiline.

Kokkuvõttes võib öelda, et sensorvõrgud ei ole loodud turvalisust silmas pidades, sellepärast avaldus ka nii palju nõrki külgi erinevatel võrgukihtidel, kuid see ei tähenda, et neid ei anna piisavalt turvata – annab küll. Tuleb lähtuda lihtsalt mõistlikkuse printsiibist – vastavalt rakenduse spetsiifikale ja andmete sensitiivsusele tuleks valida turvatse ja –meetmed.

Kasutatud kirjandus

[1] A. Stubblefield, J. Ioannidis, and A. Rubin. A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). *ACM Transactions on Information and System Security* (2004) lk 319-332.
[2] V. Moen, H. Raddum, and K. J. Hole. Weaknesses in the temporal key hash of WPA. *SIGMOBILE Mobile Computing and Communications Review* (2004) lk 76-83.
[3] W. Xu. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. *MobiHoc '05: Proc. 6th ACM Int'l. Symp. Mobile Ad Hoc Net. and Comp.* (2005) lk 46–57.
[4] W. Xu, K. Ma, W. Trappe, and Y. Zhang. Jamming Sensor Networks:Attack and Defense Strategies. IEEE Network (May/June 2006) lk 41-47.
[5] S. Datema. A Case Study of Wireless Sensor Network Attacks. Master's Thesis in Delft University of Technology (2005).
[6] C. Karlof, N. Sastry, D. Wagner. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks.(2004) http://www.cs.berkeley.edu/~daw/papers/tinysec-sensys04.pdf.
[7] E. Biham, A. Biryukov, O. Dunkelman, E. Richardson, and A. Shamir. Initial Observations on Skipjack: Cryptanalysis of Skipjack-3XOR. *SAC '98: Proceedings of the Selected Areas in Cryptography* (1999) lk 362-376.
[8] E. Biham, A. Biryukov, and A. Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. *Lecture Notes in Computer Science* (1999) lk 12-23.
[9] J. R. Douceur. The Sybil Attack. *Proc. 1st Int.Workshop on Peer-to-Peer Systems (IPTPS)* (2002).
[10] Q. Zhang, P. Wang, D. S. Reeves, and P. Ning. Defending against Sybil Attacks in Sensor Networks. *Proceedings of the Second International Workshop on Security in Distributed Computing Systems (SDCS) (ICDCSW'05) - Volume 02* (2005) lk 185-191.
[11] B. Xiao, B. Yu. Identify suspect nodes in selective forwarding attacks. *Journal of Parallel and Distributed Computing* (2007) lk 1218-1230.
[12] J. Newsome, E. Shi, D. Song and A. Perrig. The Sybil Attack in Sensor Networks: Analysis and Defenses. *Proceedings of the Third International Symposium on Information Processing in Sensor Networks* (2004) lk 259-268.
[13] B. Deb, S. Bhatnagar, and B. Nath. ReInForM: Reliable Information Forwarding Using Multiple Paths in Sensor Networks. *Proc. 28th Annual IEEE Int'l. Conf. Local Computer Networks (LCN 2003)*.
[14] D. Ganesan, R. Govindan, S. Shenker, D.Estrin. Highly Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks. *ACM SIGMOBILE Mobile Computing and Communications Review* (2002), lk 10-24.
[15] T. Aura, P. Nikander, and J. Leiwo. DOS-Resistant Authentication with Client Puzzles. *Proc. Security Protocols Workshop 2000*, (2000), lk 170-177.
[16] A. Wood and J. Stankovic. Denial of Service in Sensor Networks. *IEEE Computer* (2002), lk 54–62.
[17] T. G. Roosta. Attacks and Defenses of Ubiquitous Sensor Networks. *Technical Report No. UCB/EECS-2008-58* (2008).